FAULT PROTECTION DESIGN FOR THE COMMAND AND DATA SUBSYSTEM ON THE CASSINI SPACECRAFT

Thomas K. Brown
James A. Donaldson

Jet Propulsion Laboratory, California Institute of Technology
Pasadena, California

ABSTRACT

The Cassini orbital mission is to explore the Saturnian system in much greater depth than was possible by the Voyager flyby missions. To do this, the Cassini spacecraft is comprised of a Saturn orbiter and a Titan probe.

The Command and Data Subsystem (CDS) on Cassini is responsible for uplink command processing, spacecraft intercommunications and control, and downlink telemetry formatting. The 10.7 year mission life, 160 minute round-trip light time, and extended periods of operation without continuous ground communications drive the CDS design in directions of redundancy, autonomy, and fault protection to accommodate the mission object ives,.

INTRODUCTION

in order to understand the fault protection design of the CDS on the Cassini spacecraft, it is first necessary to understand the basic mission and spacecraft design. This is the purpose of the following two sections.

CASSINI MISSION

The Cassini mission is to provide in-depth exploration of the Saturnian system, This includes the planet itself, its rings and magnetosphere, the moon Titan, and eight icy satellites. Launch is set for October 1997. The trajectory to Saturn will take 6.7 years and require two Venus and one Earth flyby gravity assists. On the trajectory to Saturn, there will be a Jupiter flyby. Once at Saturn in June 2004, the spacecraft will perform a Saturn Orbit Insertion (S01) maneuver and will orbit the planet for four years, until June 2008. This will provide a 60 orbit tour that includes 33 Titan flybys. During the first or second flyby, the Titan probe will be released to study the atmosphere of the satellite. On some of the remaining Titan flybys, the spacecraft's synthetic aperture radar (SAR) will be used to penetrate the obscuring atmosphere of Titan to take Magellan type, SAR images of its surface,

Cassini Mission Design

The spacecraft is relatively quiescent for the first 6.7 years during its cruise to Saturn and is in communication with Earth usually only once per week, Uplink commanding is limited to the following rates in bits per second (bps): 7.8125, 15.625, 31.25, 62.5, 125, 250, and 500. While in orbit around Saturn, the spacecraft will collect science data for sixteen hours and then will point the high gain antenna at the earth to downlink the data at a ninety day optimized rate for eight hours. There are eight in-flight downlink rates that range from 5 to 165,900 bps. In order to accommodate data collection while not being able to downlink to Earth, the spacecraft can store up to four gigabits of data on board.

This mission makes it necessary to operate the spacecraft in three modes:

Normal,
Mission critical, and
Safing critical.

I'he normal mode occupies almost all of the mission and all spacecraft functions or services must be provided in order to achieve the objectives involved in the cruise to and orbits around Saturn. The mission critical mode mandates only those services necessary to operate the spacecraft during Critics] sequences (Launch, S01, and Titan Probe Relay). This mode is termed "mission critical" because these sequences are one time events that must be completed for the mission to succeed. The final mode, safing critical, occurs after the spacecraft has suffered a service interfering fault and is required to be placed into a safe, quiescent configuration for ground intervention.

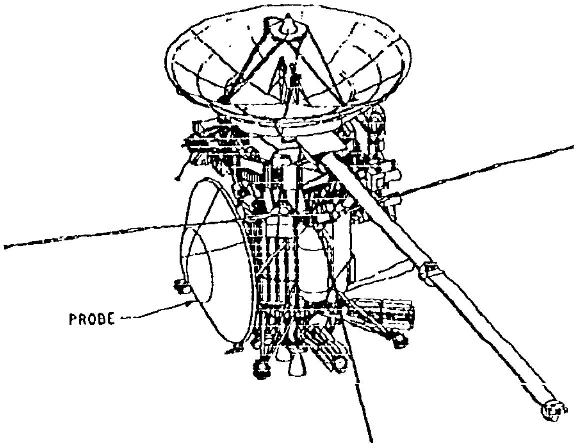


Figure 1 Cassini Spacecraft Configuration

CASSINI SPACECRAFT

The Cassini spacecraft shown in Figure 1 is approximately 5,75 meters (m) high, 4.5 m across, and has a mass of nearly 4,637 kilograms (kg) (1,925 for the spacecraft, 312 for the probe, and 2,400 for fuel). It carries three radioisotope thermoelectric generators (RTGs) capable of producing between 825 and 650 watts over the mission. The Cassini spacecraft is somewhat unique in that it has no articulated platforms. The spacecraft must orient itself in order to point any directional device, e.g. cameras and antennas.

Cassini's payload is twelve science instruments and a Titan probe. The twelve instruments are made up of four optical remote sensing science instruments, six fields, particles and waves science instruments, and two microwave remote sensing science instruments.

Cassini Spacecraft Avionics Architecture

The spacecraft's avionics architecture is shown in Figure 2. This viewpoint is from an end-to-end uplink command reception to downlink telemetry transmission. Ground operations are not included in the figure.

The spacecraft contains six major subsystems:

1 Radio Frequency Subsystem (RFS) - uplink command reception and downlink telemetry transmission,

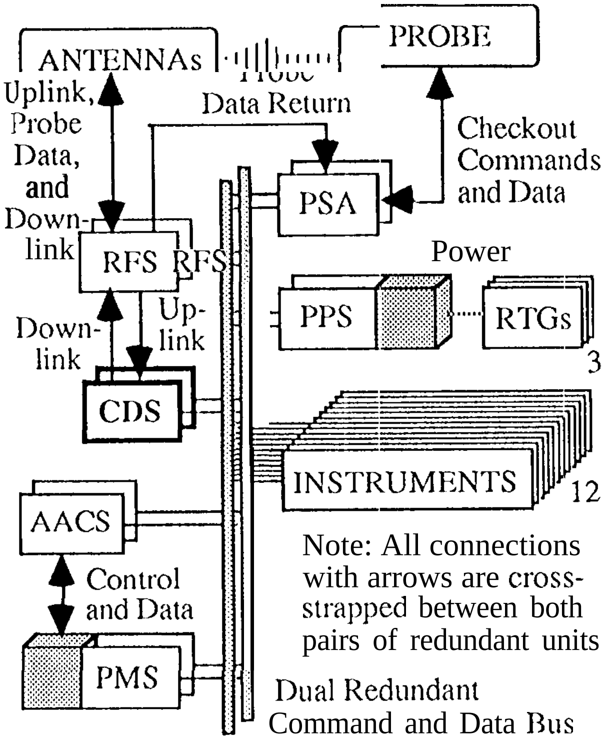
2 Command and Data Subsystem (CDS) - uplink command processing, spacecraft intercommunication, and downlink telemetry collection and packetization,

3 Attitude and Articulation Control Subsystem (AACS) - attitude determination, attitude control, thrust vector control, and main engine control,

4 Propulsion Module Subsystem (PMS) - propellant tanks, thrusters, and main engines for spacecraft maneuvers (controlled by AACS),

5 Power and Pyrotechnics Subsystem (PPS) - power supply, conditioning, and control along with pyrotechnic firing circuitry, and

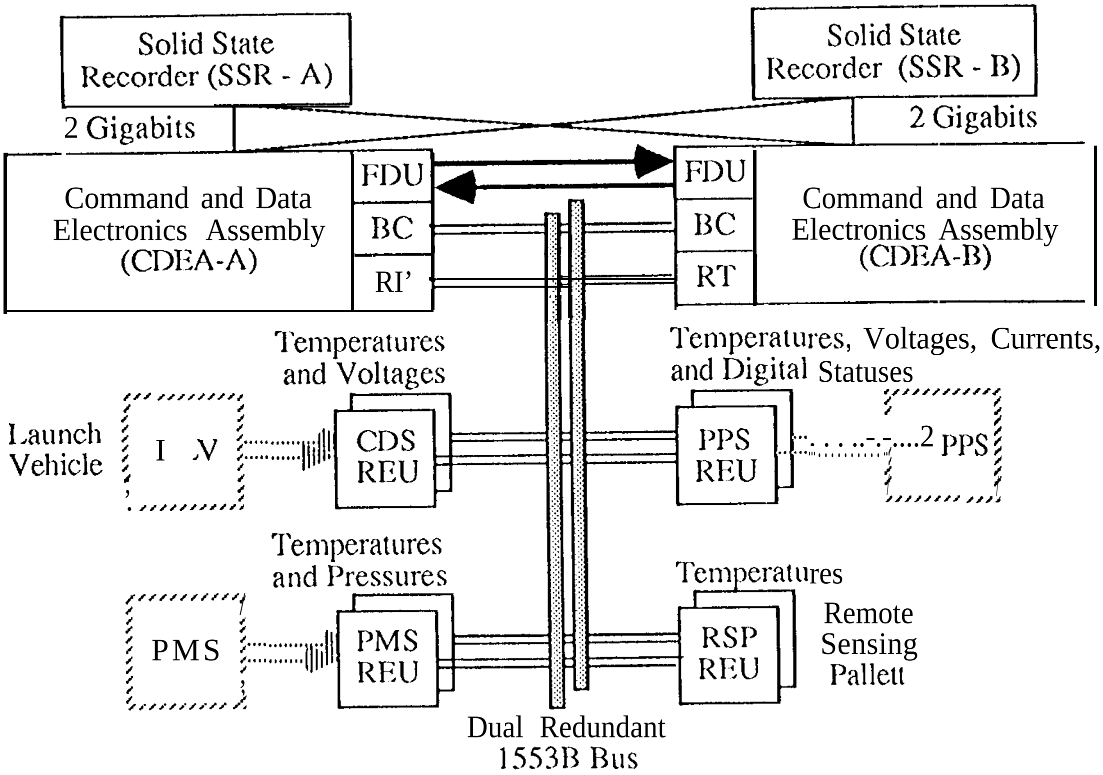
6 Probe Support Avionics (PSA) - probe checkout during cruise and data return during probe Titan entry.



Note: All connections with arrows are cross-strapped between both pairs of redundant units

Figure 2 Cassini Functional Block Diagram

The RFS, CDS, and AACS are completely dual redundant. The RFS operates with only one unit powered. The CDS and AACS must operate with either both units or one unit powered (one unit cold-spared). The PPS and PMS have redundant communication interfaces, but each contains nonredundant elements, This was done because competing factors such as mass, power, and volume resulted in some monolithic design and some duplicity of function replacing multiplicity of elements, i.e. functional redundancy replacing physical redundancy. This is shown by gray shading in Figure 2 and by dashed lines in Figure 3.



Solid State Recorder (SSR - A)
Solid State Recorder (SSR - B)
2 Gigabits
2 Gigabits
Command and Data Electronics Assembly (CDEA-A)
FDU
BC
RI'
FDU
BC
RT
Command and Data Electronics Assembly (CDEA-B)
Temperatures and Voltages
Temperatures, Voltages, Currents, and Digital Statuses
Launch Vehicle
I .V
CDS REU
PPS REU
2 PPS
Temperatures and Pressures
Temperatures
PMS
PMS REU
RSP REU
Remote Sensing Pallett
Dual Redundant 1553B Bus

Figure 3 Cassini Command and Data Subsystem Functional Block Diagram

THE COMMAND AND DATA SUBSYSTEM

The CDS is the hub of communications within the spacecraft and between the spacecraft and the ground. It provides a set of services that is supported by a dual redundant architecture.

CDS Architecture

The architecture of the CDS is shown in Figure 3. There are four primary regions associated with the CDS:

1 One set of Command and Data Electronics Assemblies (CDEAs),
2 One set of Solid State Recorders (SSRs),
3 Four sets of Remote Engineering Units (REUs), and
4 One set of MIL-STD-1553B buses (CDS Buses).

The CDEAs are referred to as the central units and the REUs, SSRs, and Buses as the peripheral units.

Each CDEA contains the following components:

1 An engineering flight computer with 512K of Random Access Memory (RAM) and 8K of Programmable Read Only Memory (PROM) for supporting CDS services and redundancy management,
2 A hardware command decoder for uplink command reception from the RFS,
3 A Reed Solomon downlink unit to encode telemetry for the RFS,
4 A timing unit for spacecraft time maintenance and synchronization signal generation,
5 A Bus Controller (BC) to manage 1553B bus activities (only one CDEA BC is active. at a time),
6 A 1553B Remote Terminal (RT) so the BC can communicate with the redundant CDEA, and
7 A Fault Detection Unit (FDU) with a special interface to the redundant CDEA to manage internal CDS redundancy of both the CDEAs and the SSRs.

The SSRS each contain about two gigabits of Dynamic Random Access Memory (DRAM) and are cross strapped to both CDEAs. The REUs are used primarily to collect engineering measurements (temperatures, pressures, voltages, currents, and digital statuses) from around the spacecraft. The CDS REU is used in addition to convey launch vehicle commands and separation indicators to the CDS, and the PPS REU is used additionally to convey commands from the CDS to the PPS. The 1553B bus provides for intercommunications between a BC and the thirty remote terminals (RTs) on the spacecraft (see Figures 2 and 3).

As can be seen, this dual redundant architecture supports single fault tolerance. Because of the power, mass, and space limitations on the spacecraft, multiple (more than two) redundancy is not realizable. As a result, the CDS must detect and respond to all single faults that can render any one unit in any of its dual redundant sets inoperable. It accomplishes this using hardware and software fault detection mechanisms coordinated through the inter-CDEA FDU signals.

Only one CDEA can be prime at any one time, meaning that it controls access to the SSRS and its BC controls the 1553B bus, The other CDEA is backup (it can access the SSR not being used by the prime CDEA but its BC is inhibited). Redundancy management is accomplished using the interface signals passing between the CDEA FDUs coupled with both PROM and RAM code residing in the CDEA.

CDS Services

The services that CDS provides areas follows:

1 Uplink Commanding - the ability to command and control the spacecraft from the ground.
2 Sequencing - the ability to store sequences of commands from the ground for later execution in order to orchestrate sets of activities. Three of these sequences are deemed critical, namely launch, SOI, and probe relay where completing the event is more crucial than the safety of the spacecraft itself.
3 Time-keeping - the ability to maintain a unique spacecraft time in order to coordinate spacecraft activities and synchronize science and engineering subsystems.
4 Downlink telemetry - the ability to provide visibility into engineering subsystem performance and science subsystem data.
5 Bulk data handling - the ability to buffer on-board data when the data collection rate exceeds the downlink telemetry rate capability.
6 Spacecraft intercommunications - the capability to communicate with the engineering and science subsystems on-board the spacecraft.
7 Control services - the capability to monitor and control on-board temperatures.
8 System Fault Protection (SFP) - the capability to host algorithms (monitors and responses) to respond to non-CDS spacecraft level faults.
9 CDS Fault Protection (CFP) - the capability to detect and respond to faults that affect the above eight services CDS provides when necessitated by the mission phase

All these services are key to the operation of the spacecraft. During certain critical mission phases, some of these services are more crucial than others.

CDS FAULT PR OTECTION

On Cassini, fault protection refers to those flight and ground based hardware, software, and procedural elements that avoid, detect, and respond to perceived spacecraft faults. It has denotations of fault intolerance and fault tolerance [1]. In the former, the goal is to prevent or minimize failure through the use of conservative design practices, etc. In the latter, the goal is to nullify the effects of failure, e.g. through the use of redundancy. Consequently, the purpose of fault protection is two fold:

1 To provide a highly reliable spacecraft that will survive the entire 10.7 year mission, and
2 To provide a highly available spacecraft for the critical events of launch, SOI, and the Probe data relay sequences.

These goals are met through the on-board, autonomous systems that ensure spacecraft system integrity in the presence of anomalous conditions coupled with ground intervention when time and circumstances permit,

CDS Fault Protection Requirements

The fundamental requirement on CDS fault protection (CFP) is one of Single Fault Tolerance (SFT). In other words, no credible Single Point Failure (SPF) shall prevent attainment of the primary mission objectives or result in a severely degraded mission. The primary mission objectives are:

1 Ability to obtain minimum essential engineering data and command capability to operate the spacecraft,
2 Successful Earth avoidance,
3 Successful targeting fOr and execution Of sol,

4 Successful Probe delivery and data return, and

5 Acquisition of science data from all except one instrument, or the acquisition of the minimum engineering data to interpret (he science data from all except one instrument.

The mission is significantly degraded if either:

1 A viable mission exists, but most of the primary mission objectives can not be met, or

2 A satisfactory mission can be accomplished, but only after substantial redesign of the mission, software, and sequences.

There are exceptions to this requirement and they are called out specifically in the Cassini single point failure exemptions list. They include such items as the misuse of uplink commands or stuck bits in interface circuitry causing CDS to enter inappropriate states or have its memory overwritten. They also include systemic design and Byzantine faults. [1].

A fundamental rule by which faults are assigned to either the spacecraft for autonomous handling or delegated to the ground for their intervention is that if the fault can be handled on the ground, then do not handle it on-board. Consequently, the set of faults that must be detected and responded to on-board are those faults that will disrupt the mission objectives listed above or that will result in a degraded mission and can not be handled within one month by the ground. [2]

In conjunction with the fundamental SFT requirement is a limitation that fault protection shall be designed assuming only one fault occurs at a time and that a subsequent fault will occur no earlier than the on-board response time of that fault, and that multiple detections occurring within the response time are symptoms of the original fault. [2]

CFP Approach

The approach to CDS fault protection is based around two concepts:

Designation and Classification.

Each error associated with the CDS is assigned a designation that specifies (he CDS service or services the error affects. The classification specifies the location and criticality of an error. The two prime categories of error classification are interfering and noninterfering, the determination being based upon the services required and not required in the current spacecraft phase. In addition, because of the nature of the CDS architecture, errors are also classified as being either central, affecting the CDEA, or peripheral, affecting the SSRs, REUs, or CDS Bus. The full structure of the Cassini CDS error classification scheme is as follows:

- Noninterfering
  - Message only
    - Central
    - Peripheral
  - Action
    - Central
    - Peripheral;
- Interfering
  - Temporary
    - Central
    - Peripheral
  - Permanent
    - Central
    - Peripheral

The second tier of classification is different for noninterfering and interfering errors. The noninterferin.g errors are classified as either being message only which means to log the error and continue, or action which in addition to logging the error requires some noninterfering response to take place. In the interfering category, the two sub-classifications are temporary and permanent. Thus, some of the peripheral errors especially can be temporary in nature and once resolved, the required CDS services can be restored. However, there is another class of errors that is permanent in nature and must be resolved by redundancy management, i.e. by switching to the redundant unit and/or safing the spacecraft.

The designation of an error to the service(s) it affects is constant and a function of the architecture of the subsystem. However, the classification, i.e. severity of an error, depends on the mission phase. Consequently, Table 1 indicates the classification of errors with different designations to mission phase. Notice that within mission critical, each critical sequence could have different service fault classifications.

CFP Design

'l-he design of the CFP follows the monitor/response approach practiced on previous JPL spacecraft. Here, a fault occurs and the system detects a breach in its intended functionality. This results in an error being generated. These errors are detected in a distributed manner by the hardware and software components of the system. Since the subsystem was designed using functional decomposition, each component's function is relevant to one or more of the CDS services.

As the error is mapped to a designation of the service that is affected and the service is mapped (o its criticality during a specific mission phase, the response to an error will adjust during the mission accordingly.

For central errors, if the fault has been determined to be interfering, the CDEA will be reset and autonomous central redundancy management will be invoked to either recoup the same CDEA or switch to the backup unit.

in the peripheral area, since the fault is external to the CDEA, resetting the CDEA will do nothing to solve the problem, The designation of the error is determined to infer its interfering classification and whether it is permanent or temporary. The basic responses to each peripheral interfering fault are as follows:

1 SSRS - Switch to a CDEA with an operational SSR.
2 REUs - REUs are handled on a set-by-set basis meaning that each redundant pair is considered separately. If one unit of a redundant pair fails, switch to the redundant unit.
3 CDS Buses - The bus is complicated by the fact that there are thirty RTs and one BC attached to it. The basic response is:
   1 If a single R"] is not responding or corrupting a bus, limit communications with it,
   2 If communications to multiple RTs is not possible on a single bus, switch buses, or
   3 If communications on both buses is lost, swap to the redundant CDEA and its BC.

All the monitors and responses have enables/disables configurable by both the ground and the spacecraft.

Acknowledgment

'l'he work described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

References

1 D. P. Siewiorek and R. S. Swarz, *Reliable Computer System Design and Evaluation,* Second Edition, Digital Press, 1992.
2 C. El, Kohlhase, "Cassini Project Policies and Requirements Document", JPL PD 699-004. July 1992 (JPL internal document).

Table 1 CDS Service Criticality to Mission Phase

item	Service	Mission Phase				
		Normal	Safing Critical	Mission Critical		
				Launch	SOI	Probe Relay
1	Uplink	x	x	o	0	0
2	Sequencing	x	o	c	c	c
3	Time-keeping	X	P	x	x	x
4	Telemetry	x	x	0	0	0
5	Bulk data handling	x	o	0	0	x
6	Spacecraft Intercom-munications	x	p	p	P	P
7	Control Services	x	x	0	0	0
8	System Fault Protection	x	x	x	x	x
9	CDS Fault Protection	x	x	x	x	x

Where **X =** required, O = not required, P = partial, and C = critical only